

EDITRAN/CF

Windows/Unix

Manual de Usuario e Instalación

INDRA

30 de octubre de 2014

1. INTRODUCCIÓN AL MÓDULO EDITRAN/CF ... 1-1
2. PROCEDIMIENTO DE FIRMA Y CIFRADO PKI ... 2-1
2.1. Firma de un fichero y verificación de la misma ... 2-1
2.2. Cifrado de un fichero y descifrado del mismo ... 2-1
3. COMPONENTES FUNCIONALES DE EDITRAN/CF ... 3-1
3.1. Esquema de componentes funcionales de EDITRAN/CF ... 3-2
3.2. Módulos de EDITRAN/CF en el componente que genera el fichero ... 3-3
3.2.1. Módulo ejecutable EDITRAN/CF ... 3-3
3.2.2. Certificado para cifrar el fichero ... 3-3
3.2.3. Certificado para firmar el fichero. ... 3-4
3.2.4. Clave privada (cifrada mediante triple DES) correspondiente al certificado para firmar. ... 3-4
3.2.5. Comando de modificación de password de la clave privada ... 3-4
3.3. Módulos de EDITRAN/CF en el componente de EDITRAN ... 3-5
3.3.1. Módulo ejecutable EDITRAN/CF ... 3-5
3.3.2. Librería dinámica de enlace EDITRAN/G-EDITRAN/CF ... 3-5
3.3.3. Certificado para descifrar el fichero ... 3-5
3.3.4. Certificado y clave privada (cifrada mediante triple DES) para descifrar. ... 3-5
4. INSTALACIÓN DEL MÓDULO EDITRAN/CF ... 4-1
4.1. Componente generador del fichero ... 4-1
4.2. Componente de EDITRAN ... 4-1
5. PARAMETRIZACIÓN DE EDITRAN ... 5-1
5.1. Parámetros EDITRAN/G ... 5-1
5.2. Detección de fichero manipulado ... 5-2
6. COMANDOS INCLUIDOS EN EDITRAN/CF ... 6-1
6.1. Comando EDItranCF ... 6-1
6.1.1. Sintaxis ... 6-1
6.1.2. Ejemplo ... 6-1
6.1.3. Retorno ... 6-2
6.1.4. Resultado ... 6-2
6.2. Comando changepass ... 6-3
6.2.1. Sintaxis ... 6-3
6.2.2. Ejemplo ... 6-3
6.2.3. Retorno ... 6-3
6.2.4. Resultado ... 6-3

1. Introducción al módulo EDITRAN/CF

EDITRAN es un conjunto de aplicaciones que permiten la transmisión de ficheros de manera segura entre entornos heterogéneos.

Sin embargo, las organizaciones que utilizan EDITRAN pueden necesitar mantener la integridad (el fichero no puede ser manipulado) y la confidencialidad (nadie puede ver el contenido del fichero) de los ficheros que ellas mismas generan incluso dentro de sus propias organizaciones.

Desde el momento en que una organización genera un fichero hasta el momento en el que es transmitido por EDITRAN, el fichero puede pasar por diferentes máquinas incluso distanciadas físicamente entre sí.

EDITRAN/CF evita el riesgo de manipulación o consulta de los ficheros generados por las organizaciones antes de ser enviados por EDITRAN.

2. Procedimiento de firma y cifrado PKI

En este apartado se explicará de manera breve y clara los procedimientos implicados en la firma y cifrado de ficheros mediante certificados digitales X509 v3 e infraestructura de clave pública PKI.

2.1. Firma de un fichero y verificación de la misma

Los pasos que se realizan para la firma de un fichero y su verificación son los siguientes:

1.- El remitente aplica un algoritmo hash a los datos y genera un valor hash.

2.- Con su clave privada, el remitente transforma el valor hash en una firma digital.

3.- A continuación, el remitente envía al destinatario los datos, la firma y el certificado del remitente.

4.- El destinatario aplica el algoritmo hash a los datos recibidos y genera un valor hash.

5.- El recipiente utiliza la clave pública del firmante y el valor hash recién generado para comprobar la firma.

2.2. Cifrado de un fichero y descifrado del mismo

Los pasos que se realizan para la firma de un fichero y su verificación son los siguientes:

1.- El remitente genera una clave simétrica aleatoria.

2.- Con la clave simétrica, el remitente cifra el contenido del fichero utilizando un algoritmo de cifrado de clave simétrica que es mucho más rápido que el de clave asimétrica.

3.- A continuación, el remitente cifra la clave simétrica con la clave pública del destinatario.

4.- El destinatario utiliza su clave privada para poder descifrar la clave simétrica.

5.- Una vez descifrada la clave, la utilizará para descifrar el fichero.

Los algoritmos hash pueden procesar los datos más deprisa que los algoritmos de claves públicas. La codificación hash de datos también reduce el tamaño de los datos que se van a firmar y, por tanto, acelera el proceso de firma. Cuando se crea o se comprueba la firma, el algoritmo de claves públicas tiene que transformar únicamente el valor de hash (128 ó 160 bits de datos).

3. Componentes funcionales de EDITRAN/CF

EDITRAN/CF tiene dos componentes funcionales. Uno situado en el lado donde se genera el fichero y otro situado en la máquina donde se encuentra EDITRAN instalado.

Los componentes utilizan Infraestructura de clave pública (PKI) utilizando los procedimientos de firma y cifrado de datos.

El primer componente, instalado en la máquina que genera el fichero, permite cifrarlo y firmarlo de manera que desde ese momento se garantiza la integridad y la confidencialidad fichero.

Se garantiza la confidencialidad porque el fichero está cifrado y únicamente EDITRAN será capaz de descifrarlo, también se garantiza la integridad porque nadie podrá manipular el fichero durante el camino.

Además EDITRAN únicamente transmitirá ficheros firmados. Para poder firmar el fichero la aplicación deberá utilizar una clave privada que se encuentra cifrada, mediante una password, utilizando un mecanismo de Triple DES. Es decir únicamente podrá firmar el que conozca la password y disponga de la clave privada necesaria.

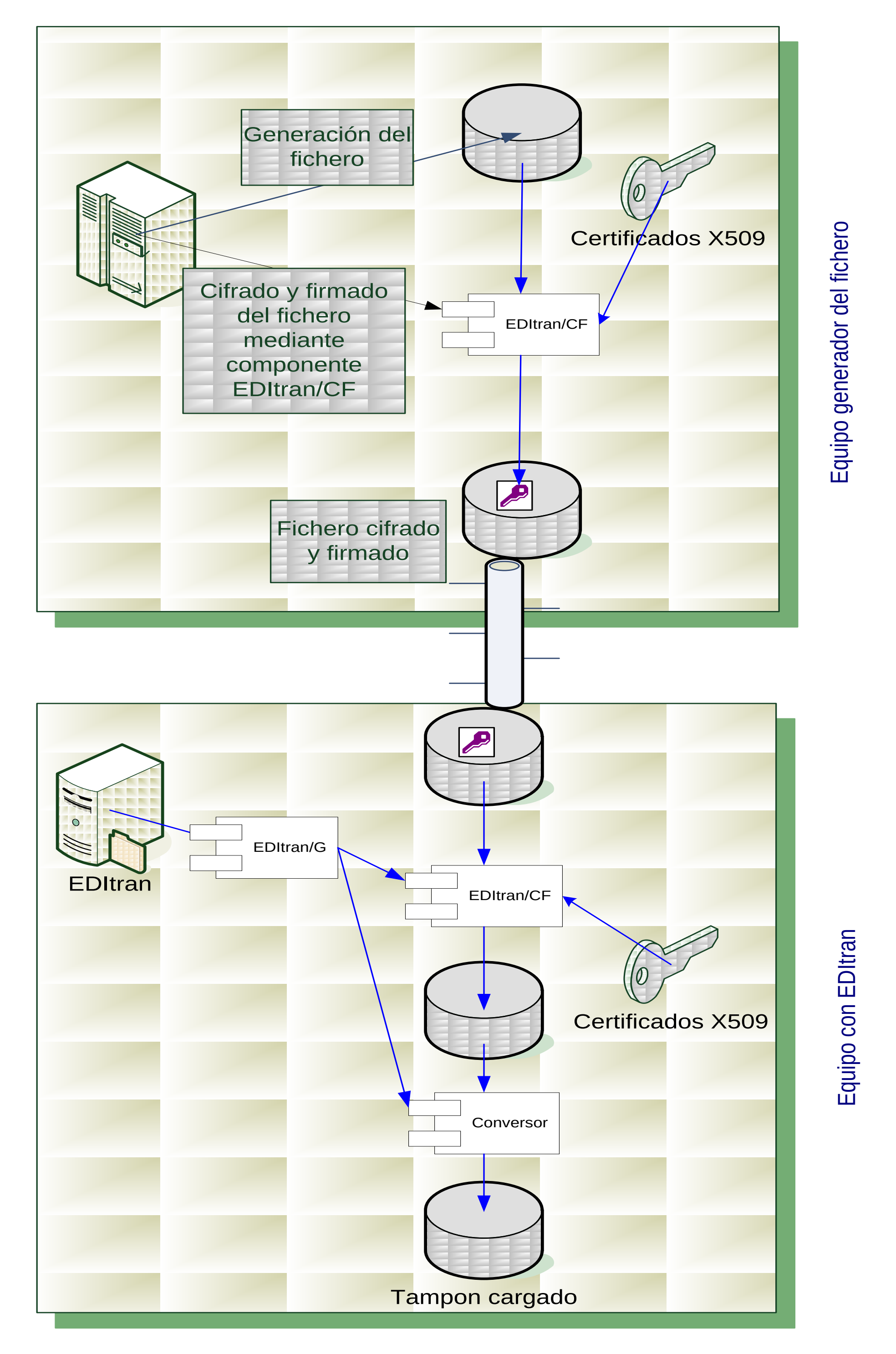
El segundo componente funcional de EDITRAN/CF está embebido en EDITRAN, de manera que antes de cargar el fichero y prepararlo para el envío, EDITRAN realiza de manera automática los siguientes procedimientos:

- Comprueba la firma del fichero. De esta manera se asegura que el fichero no ha sido modificado.
- Descifra el fichero.
- Carga el fichero en claro y prepara el envío.

De esta manera, sin ninguna intervención, EDITRAN verifica que el fichero no ha sido manipulado y se prepara a transmitirlo a la entidad receptora del mismo.

3.1. Esquema de componentes funcionales de EDITRAN/CF

En el esquema se encuentran separados en los dos componentes funcionales que componen EDITRAN/CF:



La aplicación de la entidad genera un fichero para ser enviado a otra entidad remota, mediante una llamada al módulo EDITRAN/CF se cifra y/o se firma el fichero. En ese momento se garantiza la confidencialidad y la integridad del mismo.

Cuando el fichero se encuentre disponible para EDITRAN, al efectuar la carga del mismo, EDITRAN comprobará su firma, descifrará el fichero y cargará el fichero en el tampón una vez descifrado.

3.2. Módulos de EDITRAN/CF en el componente que genera el fichero

Los módulos necesarios en el componente que genera el fichero son los siguientes:

- Módulo ejecutable EDITRAN/CF
- Certificado para cifrar el fichero
- Certificado para firmar el fichero
- Clave privada (cifrada mediante triple DES) correspondiente al certificado para firmar.
- Comando de modificación de password de la clave privada.

A continuación se explicará brevemente la utilidad de cada uno de los componentes.

3.2.1. Módulo ejecutable EDITRAN/CF

El modulo ejecutable de EDITRAN/CF en el componente que genera el fichero es un comando que tiene la funcionalidad de realizar una firma y/o cifrar un fichero utilizando PKI (Ver apartado 2).

Mediante una serie de parámetros, el comando cifra y/o firma un fichero utilizando los certificados y claves privadas incluidas como módulos de EDITRAN/CF.

Para más información de utilización y códigos de retorno del comando, consulte el apartado 6(Comandos incluidos en EDITRAN/CF).

3.2.2. Certificado para cifrar el fichero

En el cifrado de claves públicas se utilizan dos claves: una pública y una privada, que se encuentran relacionadas matemáticamente.

Para diferenciarlo del cifrado de claves simétricas, en ocasiones el cifrado de claves públicas también se denomina cifrado de claves asimétricas. En el cifrado de claves públicas, la clave pública puede intercambiarse libremente entre las partes o publicarse en un repositorio público. Sin embargo, la clave privada seguirá siendo privada. Los datos cifrados con la clave pública sólo pueden descifrarse con la clave privada. Los datos cifrados con la clave privada sólo pueden descifrarse con la clave pública. El remitente tiene la clave pública del destinatario y la utiliza para cifrar un mensaje, pero sólo el destinatario tiene la clave privada relacionada que se utiliza para descifrar el mensaje.

Los algoritmos de clave pública son ecuaciones matemáticas complejas en las que se utilizan cifras muy altas. Su principal inconveniente es que proporcionan formas relativamente lentas de criptografía. En la práctica, se utilizan generalmente sólo en situaciones críticas, como en el intercambio de una clave simétrica entre entidades o para la firma de un hash de un mensaje (un hash es un resultado de tamaño fijo que se obtiene mediante la aplicación a los datos de una función matemática unidireccional, denominada algoritmo ***HASH***).

El uso de otras formas de criptografía, como la criptografía de claves simétricas, junto con la criptografía de claves públicas optimiza el rendimiento. El cifrado de claves públicas proporciona un método eficiente para enviar a otra persona la clave secreta que se utilizó cuando se realizó una operación de cifrado simétrico sobre una gran cantidad de datos.

EDITRAN/CF necesita un certificado que se utilizará para obtener la clave pública RSA del receptor y poder cifrar el fichero. El proceso de cifrado asimétrico es un proceso que implica cálculos matemáticos complejos que retardarían demasiado en proceso de cifrado, por esa razón, para cifrar se suelen utilizar claves simétricas. EDITRAN/CF calcula una clave simétrica aleatoria y cifrará el fichero mediante un algoritmo de clave simétrica (Triple DES). A su vez la clave simétrica es cifrada con la clave pública RSA asimétrica del receptor y enviada al receptor para que éste, después de descifrarla con su clave privada, pueda descifrar el fichero.

3.2.3. Certificado para firmar el fichero.

Una firma digital es un medio para que los creadores de un mensaje, archivo u otra información codificada digitalmente vinculen su identidad a la información; es decir, proporcionen una firma.

El proceso de firma digital de información implica la transformación de la información y de otros datos secretos del remitente en una etiqueta denominada firma. Las firmas digitales se utilizan en entornos de claves públicas para ayudar a asegurar las transacciones de comercio electrónico al comprobar que la persona que envía el mensaje es realmente quien dice ser y confirmar que el mensaje recibido es idéntico al mensaje enviado.

Con frecuencia, las firmas digitales se utilizan cuando los datos se distribuyen como texto no cifrado, como ocurre con el correo electrónico. En este caso, y aunque la confidencialidad del mensaje no garantiza el cifrado, puede ser importante para asegurar que los datos se encuentran en su forma original y que no ha sido un impostor quien los ha enviado.

Un hash, también denominado valor hash o síntesis del mensaje, es un tipo diferente de transformación de datos a partir de criptografía basada en claves (ya sean simétricas o públicas).

Un hash es la conversión de determinados datos de cualquier tamaño, en un número de longitud fija no reversible, mediante la aplicación a los datos de una función matemática unidireccional denominada algoritmo hash. La longitud del valor hash resultante es tan grande que las posibilidades de encontrar dos datos determinados que tengan el mismo valor hash son mínimas. El remitente genera un algoritmo hash del mensaje, lo cifra y lo envía junto con el mensaje. A continuación, el destinatario descifra tanto el mensaje como el hash, produce otro hash a partir del mensaje recibido y compara los dos hash. Si son iguales, es muy probable que el mensaje se transmitiera intacto.

Puede utilizar tecnología de claves públicas junto con algoritmos hash para crear una firma digital. Una firma digital actúa como una comprobación de integridad de datos y proporciona una prueba de posesión de la clave privada

3.2.4. Clave privada (cifrada mediante triple DES) correspondiente al certificado para firmar.

Como se ha explicado, para firmar el hash del fichero, es necesaria, además de un certificado, la utilización de una clave privada asociada a la clave pública de ese certificado.

La clave privada está cifrada mediante una password para que únicamente el conocedor de la password sea capaz de firmar el fichero.

3.2.5. Comando de modificación de password de la clave privada

Como ya se ha comentado la clave privada se encuentra cifrada mediante un algoritmo de Triple DES y una password. Este comando modifica la password con la que se encuentra cifrada la clave privada.

Para realizar el proceso de modificación de password, es necesario que se aporte la password a modificar ya que el comando descifrará la clave privada utilizando la password antigua y la volverá a dejar cifrada con el algoritmo simétrico Triple DES mediante la nueva password.

3.3. Módulos de EDITRAN/CF en el componente de EDITRAN

Los módulos necesarios en el lado donde reside EDITRAN son los siguientes:

- Módulo ejecutable EDITRAN/CF
- Librería dinámica de enlace EDITRAN/G-EDITRAN/CF
- Certificado para descifrar el fichero
- Clave privada (cifrada mediante triple DES) correspondiente al certificado para descifrar.

A continuación se explicará brevemente la utilidad de cada uno de los componentes.

3.3.1. Módulo ejecutable EDITRAN/CF

Consultar el apartado **3.2.1 Módulo ejecutable EDITRAN/CF**.

3.3.2. Librería dinámica de enlace EDITRAN/G-EDITRAN/CF

EDITRAN/G debe confirmar que el fichero no ha sido manipulado para eso necesita invocar al comando EDItranCF.

Para que EDITRAN/G pueda invocar a EDITRANCF necesita una librería dinámica (denominada EDItranFF.dll). La librería dinámica editranff.dll se incluye junto con la instalación de EDITRAN, sin embargo hay que sustituir la que instala EDITRAN por la suministrada con la instalación de EDITRAN/CF, de esta manera se verificarán la firma y se descifrará el fichero mediante EDITRAN/CF.

3.3.3. Certificado para descifrar el fichero

Para poder descifrar el fichero, se debe utilizar el certificado y su la clave privada correspondiente a la clave pública con la que se cifró (ver apartado 3.2.2, Certificado para cifrar el fichero).

3.3.4. Certificado y clave privada (cifrada mediante triple DES) para descifrar.

La clave privada del receptor se utilizará para descifrar la clave simétrica Triple DES con la que se ha cifrado realmente el fichero. Una vez obtenida la clave simétrica se procede a descifrar el contenido del fichero.

La clave privada del receptor usada para descifrar, se encuentra cifrada bajo una password conocida únicamente por EDITRAN. De esta manera nadie podrá, excepto EDITRAN, descifrar el fichero a transmitir.

4. Instalación del módulo EDITRAN/CF

4.1. Componente generador del fichero

El conjunto de componentes se envían empaquetados en un fichero ***tar***.

Para desempaquetarlos hay que ejecutar la siguiente sentencia:

```
tar xvf editrancf.tar.gz
```

Una vez desempaquetados los componentes, podemos ver como se ha creado el comando ***editrancf*** (ver apartado 3.2.1, Módulo ejecutable EDITRAN/CF)y un directorio llamado ***certificados***. El directorio *certificados* contiene 3 ficheros: dos ficheros que contienen los certificados (ver sección 3.2.2, Certificado para cifrar el fichero y 3.2.3, Certificado para firmar el fichero.) y un fichero con extensión ***pem*** (ver sección 3.2.4, Clave privada (cifrada mediante triple DES) correspondiente al certificado para firmar.) que contiene la clave privada.

4.2. Componente de EDITRAN

El conjunto de componentes se envían empaquetados en un fichero ***zip***. Se deberá descomprimir el contenido del fichero en el directorio de instalación de EDITRAN.

Se creará el comando ***editrancf*** (ver sección 3.3.1, Módulo ejecutable EDITRAN/CF) , el certificado para descifrar (ver sección 3.3.3, Certificado para descifrar el fichero), la clave privada para descifrar (ver apartado 3.3.3, Certificado para descifrar el fichero) y la librería dinámica de enlace con EDITRAN/G ***editranff.dll*** (ver apartado 3.3.2, Librería dinámica de enlace EDITRAN/G-EDITRAN/CF).

La librería dinámica ***editranff.dll*** ya existe en el directorio de instalación de EDITRAN. Deberá ser sustituida por la que se incluye en el fichero ***zip***.

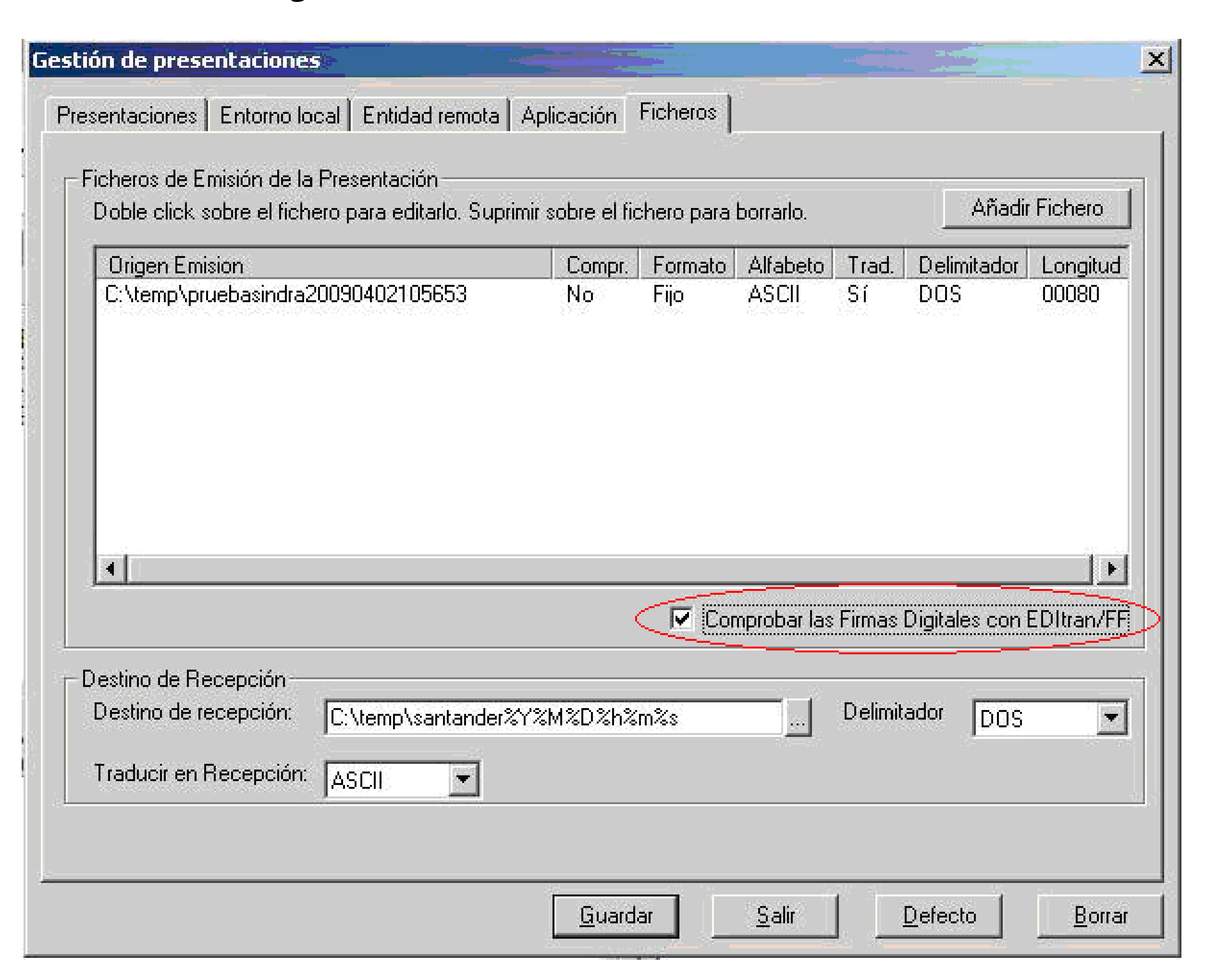
5. Parametrización de EDITRAN

Una vez instalado los módulos del componente de EDITRAN, se debe parametrizar de manera que EDITRAN pueda llamar al módulo EDITRAN/CF para que verifique la firma y se descifre el fichero a transmitir.

Además es importante conocer que ocurre cuando la verificación o el descifrado del fichero no ha sido posible y como obtener información y detalle del problema.

5.1. Parámetros EDITRAN/G

Para que EDITRAN/G lance una llamada a EDITRAN/CF y descifre el fichero y verifique su firma basta con señalar el *checkbox* ***Comprobar las Firmas Digitales con EDItran/FF*** que se encuentra en la pestaña ***Ficheros*** del dialogo de ***Gestión de presentaciones*** de la interfaz de EDITRAN/G ***menug***.

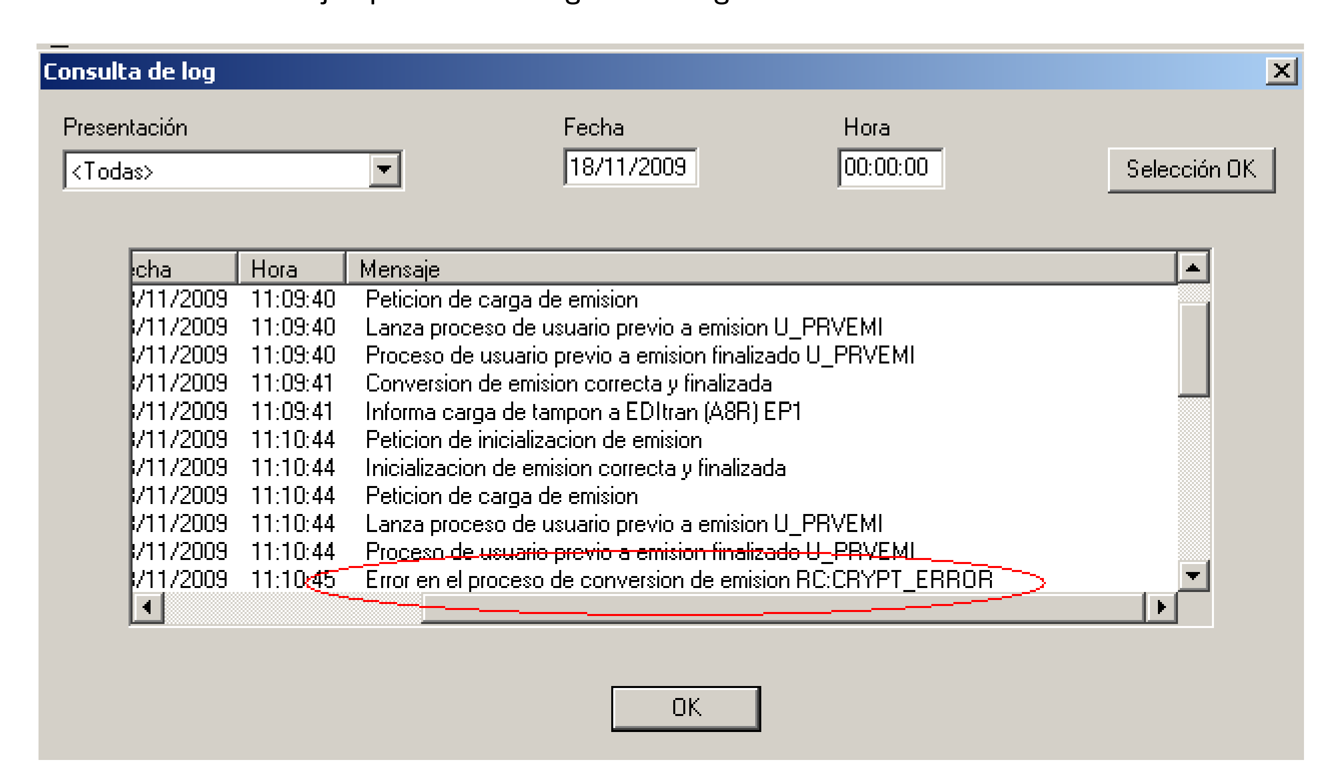


5.2. Detección de fichero manipulado

Si EDITRAN/G no ha podido descifrar el fichero o bien la firma del mismo no es correcta el proceso de carga del tampón de EDITRAN/G se interrumpirá con el siguiente mensaje:

Error en el proceso de conversión de emisión.

Este mismo mensaje aparece en el log del menug:



Para ver el detalle de lo que ha ocurrido es necesario ver el fichero ***editrang.out***.

```
################################################################################
SCRIPT DE USUARIO PREVIO A EMISION: U_PRVEMI.
Wed Sep 30 10:13:44 2009
PRESENTACION : E-"MONTILLA" (000123450-000099990-PRUEBA)
RESULTADO    : E-0000
################################################################################
Error al verificar el PKCS#7.
3992:error:04077068:rsa routines:RSA_verify:bad signature:.\crypto\rsa\rsa_sign.c:218:
3992:error:21071069:PKCS7 routines:PKCS7_signatureVerify:signature
failure:.\crypto\pkcs7\pk7_doit.c:961:
3992:error:21075069:PKCS7 routines:PKCS7_verify:signature failure:.\crypto\pkcs7\pk7_smime.c:297:
Error al validar la firma del fichero: C:\mercedes\out2tocado.p7b.
18/11/2009 11:12:28.718 (3792) .
  Modulo .\conver41.c (388)    errno = 2. No such file or directory.
18/11/2009 11:12:28.718 (3792) No tiene permiso para transmitir la presentacion.
EDItranCF:La verificación de la firma de C:\mercedes\out.p7b es correcta.
EDItranCF:La verificación de la firma del fichero C:\mercedes\out2tocado.p7b ha fallado (nRet:35).
Se cancela la carga de los ficheros.
```

6. Comandos incluidos en EDITRAN/CF

6.1. Comando EDItranCF

El comando EDItranCF contiene la funcionalidad de cifrado, firma, verificación de firma y descifrado de un fichero.

En este apartado se verán todos los parámetros del comando y lo códigos de retorno del comando.

6.1.1. Sintaxis

El comando EDItranCF tiene la siguiente sintaxis:

```
EDItranCF -r<OPER> -c<PATH_CERT_CIFRAR> -f<PATH_CERT_FIRM> -p<PASS>
                 -i<FICHERO_IN> -o<FICHERO_OUT> -n<CN> -d<PATH_CERT_DESC> -s
Siendo:
        <OPER>: Operacion a realizar. Debe ser una de las siguientes:
                c : Cifrado de <FICHERO_IN>
                f : Firma de <FICHERO_IN>
                cf: Cifrado y firmado de <FICHERO_IN>
                v : Verificaci¾n de firma de <FICHERO_IN>
                d : Descifrado de <FICHERO_IN>
                vd: Verificaci¾n de firma y descifrado de <FICHERO_IN>
        <PATH_CERT_CIFRAR>: Path del certificado usado para cifrar.
        <PATH_CERT_FIRM>: Path del certificado usado para firmar.
        <PASS>: (Opcional) Password de la clave privada.
        <FICHERO_IN>: Fichero de entrada.
        <FICHERO_OUT>: Fichero de salida.
        <CN>: (Opcional) Campo CN del DN del certificado a validar.
        <PATH_CERT_DESC>: Path del certificado usado para descifrar.
        -s: Modo silencioso.
```

6.1.2. Ejemplo

Para generar un fichero cifrado y firmado la invocación del comando será la siguiente:

```
EDItranCF -rcf -ccertificados/editran.cer -fcertificados/firmaeditran.cer -peditran -iin -oout.p7b
```

Mediante el primer argumento (***-rcf***) indica que la operación a realizar será un cifrado y una firma.

El segundo argumento (**-cccertificados/editran.cer**) indica donde se encuentra el certificado para cifrar.

El tercer argumento (***-fcertificados/firmaeditran.cer***) indica donde se encuentra el certificado para firmar.

El cuarto argumento (***-peditran***) determina la *password* con la que está cifrada la clave privada utilizada para firmar.

El quinto argumento (***-iin***) indica el fichero que se desea cifrar y firmar (en este caso se llama ***in***).

El sexto argumento (***-oout.p7b***) indica el fichero que se generará cifrado y firmado (en este caso se llama ***out.p7b***).

6.1.3. Retorno

A continuación se listarán los códigos de retorno del comando ***editrancf***.

Retorno	Explicación
1	**No se ha podido cargar el certificado para cifrar**
2	**No se ha podido cargar el certificado para firmar**
3	**No se ha podido cargar la clave privada necesaria para firmar**
4	**No se ha podido cargar el certificado para cifrar**
5	**No se ha podido cargar la clave privada necesaria para descifrar**
10	**Los parámetros suministrados al comando no son correctos**
11	**No se ha podido leer el fichero a cifrar**
12	**Error al cifrar datos**
13	**Error al pasar al formato PKCS#7**
14	**Error al guardar el fichero cifrado**
21	**Error al leer el fichero a firmar**
22	**Error al firmar datos**
23	**Error al guardar el fichero firmado**
31	**Error al leer el fichero cifrado/firmado**
32	**Error al obtener el certificado con el que se ha firmado**
33	**Verificación de firma incorrecta**
34	**El atributo Common Name del certificado firmante no es el correcto.**
35	**Error al verificar el fichero cifrado/firmado**
36	**Error al guardar el fichero en claro**
41	**Error al leer el fichero cifrado**
42	**Error al descifrar datos**
43	**Error al guardar el fichero descifrado**
90	**Licencia incorrecta**
0	**El comando ha finalizado correctamente**

6.1.4. Resultado

La ejecución del comando genera un nuevo fichero. El fichero generado tiene la estructura de un ***PKCS#7*** estándar y por tanto podrá ser validado por cualquier software compatible con éste estándar.

6.2. Comando changepass

Este comando permite la modificación de la password con el que está cifrada una clave privada.

6.2.1. Sintaxis

El comando ***changepass*** tienen la siguiente sintaxis:

```
changepass -c<CLAVE_PRIVADA> -p<PASSWORD> -n<NEW_PASSWORD>
Siendo:
        <CLAVE_PRIVADA>: Path del fichero con la clave privada.
        <PASSWORD>: Password actual con la que esta cifrada la clave privada.
        <NEW_PASSWORD>: Nueva password.
```

6.2.2. Ejemplo

Para cambiar la clave actual de "editran" por "indra", la invocación del comando será la siguiente:

```
changepass -ccertificados/ editran.cer.pem -peditran -nindra

Con el primer parámetro(-c) se indica el path donde se encuentra el fichero con la clave
privada cifrada.
El segundo parámetro (-p) indica la password con la que está cifrada la clave privada.
Con el tercer parámetro (-n) se indica la nueva password con la que quedará cifrada la
clave privada.
```

6.2.3. Retorno

A continuación se listarán los códigos de retorno del comando ***changepass***.

Retorno	Explicación
10	**No se ha podido leer la clave privada. Parámetros.**
11	**Error al crear el fichero de clave privada cifrado con la nueva password**
12	**Error al escribir el fichero de clave privada cifrado con la nueva password**
0	**No se ha podido cargar el certificado para cifrar**

6.2.4. Resultado

La ejecución del comando modifica la password con la que se cifra, mediante Triple DES, una clave privada.



Centros de Competencia eCommerce

Avda. de Bruselas 35
28108 Alcobendas.
Madrid, España
T. +34 91 480 80 80
T. +34 91 480 50 00
www.indracompany.com